WHITE PAPER

SYSTEM IMPLEMENTATION CONSIDERATIONS FOR PAYMENT TRANSPARENCY

Elbin Elias

Infosys®
Navigate your next

Abstract

Amidst fears of banks being used as vehicles for financial crime, international organizations are asking banks to enhance the monitoring of international payments, which are the payments initiated by them or where they act as an intermediary in the chain of payments. The basic area of focus amongst others like KYC, is the quality in the completeness and correctness of the payment message itself that gets transmitted to effect the payment. This paper focuses on the importance of payment transparency, the related international regulatory guidelines, how they impact design of the systems in the end-to-end payment chain and the implementation of the same for one of the SWIFT message formats, namely MT103.

Introduction

With the advent of XML-based messaging, payment messages are able to hold more and more data related to payments vis-à-vis the traditional MT, EDI or other traditional and proprietary formats. The payment transformation and payment processing engines in the back offices that have not migrated yet to the new messaging standards cannot accept the additional data provided resulting in loosing relevant/ additional payment information while forwarding further to a clearing or another bank for further processing. This brings in several issues:

- Lack of information on the parties to a payment – There is less information on the ultimate debtor / creditor rather than just the intermediaries in the chain of transfer.
- Lack of traceability – Financial system is used for money laundering, terrorist funding, and other forms of financial crime.

Added to the technological limitations are the gaps in the current business operations related to KYC norms and legacy corporate partnerships that have not undergone changes in terms of the amount and quality of data captured for the transfer of funds.

The basis for the payment transparency requirements are the comprehensive, enhanced, and consistent framework of measures for combating terrorist financing and money laundering, specified as part of the Financial Task Action Force's (FATF) 2012 recommendations, mainly the Recommendation 16. This specifies the need for the financial institutions to provide the information on the ultimate beneficiary and originator and to monitor the quality of data in the transactions they process. Several countries (FATF members) have issued regulations that reflect Recommendation 16.

Background

There are various remitter models when it comes to payments undertaken by a financial institution. Among them, the payments on behalf of another Non-FI or FI is where the information lies outside the control of a financial institution servicing the payment. Knowing who is ultimately receiving and sending the funds forms an essential part of dealing with fraud, money laundering, terrorist financing, and other forms of financial crime. Much of the data gets lost when there are multiple parties to the payment chain adding to the risk of a possible financial crime. For example in the case of an on-behalf-of payment, when the sender of the payment is marked as a bank customer, where the payment is actually done on behalf of one of the clients of the bank customer, puts the bank processing the payment at risk of being used as a vehicle for fraudulent transactions.

With a more increased need to combat terrorist organizations and other bodies of crime, banks are asked by the regulators in the countries they operate in, to increase the monitoring of international and domestic payments. For the banks, the demand for dealing with issues related to money being routed from or to the wrong hands comes together with the requirement to offer a quick, seamless, efficient, and cost-effective means for the transfer of funds. This stresses on the need to have quality information in the messages used to transfer funds. Understanding the key data in the payment process enables scrutiny in an automated way of the legitimacy in the transfer of funds.

FATF Recommendation 16

FATF has over the years kept the recommendations on the international standards to combat money laundering and the financing of terrorism and proliferation up to date. It is done with the intention of staying updated with the latest mechanisms used to put the financial system to illegal use. Even though there are 40 recommendations focusing on the said areas, it is the recommendation 16 that emphasizes the requirements for wire transfers. Member countries have created their own regulations on the basis of FATF recommendations that cater to the geographical specifics.

Recommendation 16 applies to cross-border and domestic wire transfers including serial and cover payments. It does not apply in cases of a payment through card for goods and services purchased and inter-bank transfers, where the parties are acting on their own behalf.

For the purpose of transparency, cross-border wire transfers require the following:

- The name of the originator
- The originator account number where such an account is used to process the transaction
- The originator's address, or national identity number, or customer identification number, or date and place of birth
- The name of the beneficiary

The requirements for domestic transfers are similar but allow for a few exceptions considering the nature of the transaction and the geography involved.

Design for Payment systems

Payment systems have a significant role in ensuring adherence to Recommendation 16. A payment system here can be regarded as any system that falls in the end-to-end chain of payment initiation, transformation, or processing.

Below we look at how each of these contribute to the payment transparency needs with respect to wire transfers.

Payments initiation

This stage needs to ensure that all necessary information is captured regarding the ordering and beneficiary party to the transfer. The details that are required vary depending on the various remitter models. The information captured should be formatted into a standard message that can be accepted by further processing systems. The idea here is to ensure that the message that is sent across captures the payment details as per the transparency requirements

Payments Transformation

Financial institutions typically have a middle layer for validation and transformation purposes, which include systems that accept payment messages through channels like SWIFT, customer gateways, and internal

payment initiation systems, before a back-office system takes up the messages for further routing or settlement. In most cases, there is a conversion from the received to an outbound format specific to a back-office system. The requirement for such systems would be to ensure that no information is lost in the transformation / enrichment and to ensure that all the payment transparency information is captured, which includes storage of the payment messages at each stage of the transformation. The systems should reject payments received without the required data. It may be the case that the payments are already sanctions-checked at this stage usually by specialized systems.

Payments Settlement / Routing

The settlement systems (payments engine) must ensure that the ordering and beneficiary information is sanctions-checked before actual settlement or routing further in the payment chain. In the cases where the messages are routed further, it must be ensured that no information is modified or omitted. In the event of technical challenges, there must be mechanisms in agreement with the next party in the chain on how the information would be retained for investigation purposes that might arise in the future.

Message formatting requirements for MT103 for payments transparency

This section gives a brief on the mapping requirements for an outgoing MT103 generated by a financial institution to effect a credit transfer. These payments can be divided into two main types, though variations among them are still possible based on the type of remitter and FX requirements. The two types are own-payments and on-behalf-of payments, the difference being that the originator is a client of the bank account holder in the case of an on-behalf-of payment.

Message data information	Tag	Description
Originator of the payment	50K 52A	Own-payment – Should contain the name, account number, and address of the bank account holder. On-behalf-of payment – Should contain the name, account number, and address of the ultimate originator. In addition, tag 52 must contain the bank account holder's account number.
Beneficiary of the payment	59 57A	The name, account number, and address of the ultimate beneficiary is contained in tag 59. Additionally tag 57 must contain the financial institution of the beneficiary.
Reference info	20 72	There are multiple tags to include the payment reference. Tag 20 can contain the sender's reference, also an end-to-end ID that is present in the final statement. Tag 70 can contain the remittance information and 72 the sender-to-receiver information for reconciliation purposes.
Intermediate financial institution	56A	These fields when present need to be mandatorily routed further in the payment chain.
Amount, currency, and exchange rate	32A 33B 36	These fields when present need to be mandatorily routed further in the payment chain.

Table 1: Mapping for an outgoing MT103

There are constraints due to the differences in the capacity of the MT messages. So, if the incoming message has the complete name and address information which is beyond what could be mapped to a MT103 message due to the limitations on the length, they need to be truncated on a risk-based approach so that there is still sufficient information for sanctions-screening.

The requirements can be further enhanced to any other payment format, merely by extending the corresponding mapping rules. These rules also govern what incoming messages need, to be accepted by the bank when acting as an intermediary in the chain of payments.

Conclusion

Banks must regard payment transparency not just as a mere regulatory requirement, but rather embrace it to avoid being used as a vehicle for propagating financial crime which could lead to heavy sanctions and reputational damage beyond repair. Ensuring quality data on the payment is primary for the effective use of sanctions, fraud, and anti-money laundering systems, which augments the capability for straight-through processing. Where an information-rich message is better in fully covering any of the risks, it is important that the systems in the chain have the capability to handle and process that kind of information. Hence what is key to have is the data that is right enough that ensures neither the data quality nor the processing speed is compromised, thereby making the payment systems more efficient and effective, and caters to the customers' and regulators' needs alike.

About the Author

Elbin Elias

Lead Consultant, Cards and Payments Practice, Infosys

Elbin has over 10 years of experience, predominantly in the domains involving collateral management, payments, and cash & liquidity management. Currently, he works as Senior Business Analyst for one of the largest global banking clients in their digital transformation program. Over the years, he has worked in business analyst and test manager roles in key projects.

He can be reached at elbin_elias@infosys.com

References

http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

For more information, contact askus@infosys.com

Infosys®
Navigate your next